1. Matroids

Definition 1. *A* ***matroid*** *is defined as an ordered pair consisting of a set E, known as the ground set, and a family of subsets of E called I, the family of independent subsets of E. These satisfy the following properties:*

- $\emptyset \in I$.
- *Every subset of an independent set is independent.*
- *If A and $B \in I$ and A is larger than B, then we may find $a \in A$ so that $\{a\} \cup B$ is an independent set.*

Note that the third property recalls the well-known theorem from linear algebra stating that all bases must have the same number of elements.

Example 1. *Let A be a matrix over a field F. Let E be the set of columns of A, and let I be the collection of subsets I of E such that the corresponding collection of column vectors are independent. Then (E, I) is a matroid, denoted M[A].*

Matroids that can be represented as such an $M[A]$ are called **representable.**

There are several equivalent definitions of matroids, although this equivalence is not obvious. For example -

Another way to define a matroid is by its bases. A **basis** of a matroid is a maximal independent set. Analogously, a **circuit** is a minimally dependent set of a matroid.

Analogously to linear algebra, all bases of a matroid must have the same number of elements. (Why is this?) This number is called the **rank** of M.

We note that either the dependent sets, the bases, or the circuits of a matroid characterize the matroid completely - their simple properties may be taken as the axioms for defining a matroid. For instance, one may define a matroid as a pair $(E, \mathcal{B})$, where $\mathcal{B}$ is a collection of bases, satisfying the following properties:

- $\mathcal{B}$ is nonempty.
- If $A \neq B \in \mathcal{B}$ and $a \in A \backslash B$, then there exists $b \in B \backslash A$ such that $A \cup \{b\} \backslash \{a\} \in \mathcal{B}$. This is known as the **basis exchange property**.

If M is a matroid on E, and $A \subset E$, then we can define a matroid on A by considering the independent subsets of A as those independent in M. There is a function $r : P(E) \to \mathbb{N}$, the **rank function** of M, for which $r(A)$ is the rank of the matroid defined on A. It has the following properties:

- For any subset A, $r(A) \leq |A|$.
- If $A \subset B$, $r(A) \leq r(B)$.
- $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

One may also use the rank function to obtain an alternative, equivalent definition of a matroid.

Exercise 1. *Can you come up with a definition of matroids using circuits?*

Let M be a matroid on E, a finite set. The **closure** $cl(A)$ of a subset A is given to be the set $cl(A) = \{x \in E : r(A) = r(A \cup \{x\}\}$. More generally, define a **closure operator** $cl : \mathcal{P}(E) \to \mathcal{P}(E)$ to be a function satisfying the following conditions:

- For all subsets X, $X \subset cl(X)$.
- For all subsets X, $cl(X) = cl(cl(X))$.
- If $X \subset Y$, $cl(X) \subset cl(Y)$.
- If $a, b \in E$ and $Y \subset E$, if $a \in cl(Y \cup \{b\}) \backslash cl(Y)$ then $b \in cl(Y \cup \{a\}) \backslash cl(Y)$.

These properties may also be taken as a definition of a matroid - every function $cl : P(E) \to P(E)$ that obeys these properties determines a matroid.

We can also define a matroid using graphs. Given a graph G, we let E be the set of edges of G, and $\mathcal{I}$ the collection of all subsets I of E so that I does not contain any cycles. We claim that this is a matroid; the matroid $M(G)$ is often called a **cycle matroid**, or **graphical matroid**.

Exercise 2. *What are the bases and circuits of a graphical matroid?*

A graphical matroid is also a representable matroid. To show this, we first make a definition:

Definition 2. *The* ***incidence matrix*** *of a graph G is a $|V| \times |E|$ sized matrix A where $A_{v,e} = 1$ if v is a vertex of the edge e, and e is not a loop. Otherwise, $A_{v,e} = 0$.*

We claim that:

Theorem 1. *Over the field $\mathbb{F}_2$, $M(G)$ is isomorphic to $M[A]$, where A is defined above.*

Proof. We wish to show that for any subset $I \subset E$, I contains cycles of G iff it corresponds to columns of A which are independent. It suffices to show that C is a minimal (by inclusion) cycle of G if and only if the corresponding columns are minimally dependent (again by inclusion).

If C is a loop, the corresponding column is the null vector. Otherwise, each vertex met by C is met by exactly two edges of C. It follows that the sum of the vectors is zero modulo two, hence the vectors are dependent. Conversely, let D be a minimally dependent collection of columns; if D is the zero column then the corresponding edge is a loop. Else the sum of the vectors in D is 0 (since we are working with $\mathbb{F}_2$). Hence there exist two 1s in the ith position for each i, and hence the corresponding edges form a cycle. $\square$